(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002182769 A**

(43) Date of publication of application: **26.06.02**

(51) Int. Cl **G06F 1/00**
G06F 12/14
G11B 20/10

(21) Application number: **2000383123**

(22) Date of filing: **12.12.00**

(71) Applicant: **HITACHI LTD**

(72) Inventor: **NAGATANI TAKESHI**

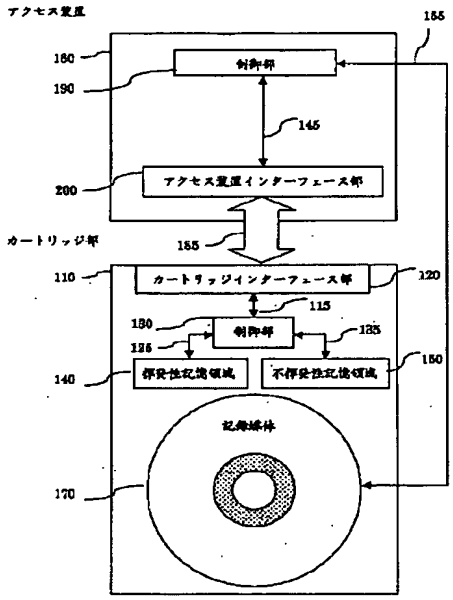
(54) **SOFTWARE AUTHENTICATING METHOD UTILIZING CARTRIDGE**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a system and a method for suppressing an illegal use of software license.

SOLUTION: The controlling part 190 of an accessing device 180 requests the controlling part 130 of a cartridge 110 to perform a software installation authentication in the case of installing software stored on a recording medium 170 inserted into the cartridge 110. The controlling part 130 authenticates the software based on authentication algorithm stored in a nonvolatile storage area 150, stores information proper to the type of machine in a volatile storage area 140 when this authentication is successful and allows the software to be installed. In the case of uninstalling the software, the controlling part 190 of the accessing device 180 requests uninstallation authentication in the same manner as the installation authentication, and the controlling part 130 allows the software to be uninstalled when the uninstallation authentication successful and erases the information proper to the type of machine stored in the storage area 140.

図 3



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－182769
（P2002－182769A）
(43)公開日　平成14年６月26日(2002.6.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　12/14	３２０Ａ	５Ｂ０１７
12/14	３２０	Ｇ１１Ｂ　20/10	Ｈ	５Ｂ０７６
Ｇ１１Ｂ　20/10		Ｇ０６Ｆ　9/06	６６０Ｄ	５Ｄ０４４

審査請求　未請求　請求項の数４　ＯＬ　（全６頁）

(21)出願番号　特願2000－383123(P2000－383123)

(22)出願日　平成12年12月12日(2000.12.12)

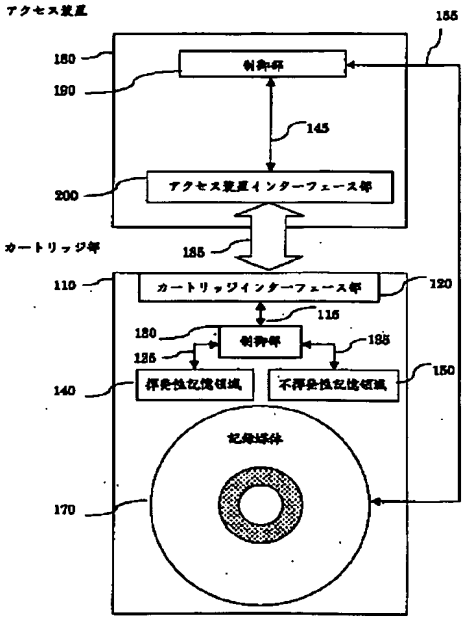
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　永谷　剛
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内
(74)代理人　100075096
弁理士　作田　康夫

Ｆターム(参考)　5B017 AA03 BA05 BB03 CA15
5B076 FB06
5D044 BC03 BC06 CC04 DE49 DE50
GK17 HL08

(54)【発明の名称】　カートリッジを利用したソフトウェア認証方法

(57)【要約】
【課題】ハードウェア及びソフトウェアの組み合わせで着脱可能な記録媒体に格納されたソフトウェアの不正インストール防止。
【解決手段】カートリッジ１１０に装着された記録媒体１７０に格納されたソフトウェアのインストールの際、アクセス装置１８０の制御部１９０はカートリッジ１１０の制御部１３０に対しソフトウェアのインストール認証要求を行う。制御部１３０は不揮発性記憶領域１５０に格納された認証アルゴリズムに基づきソフトウェアの認証を行い、成功時に揮発性記憶領域１４０に機種固有情報を格納してインストールを許可する。ソフトウェアのアンインストールの際アクセス装置１８０の制御部１９０はインストール時と同様アンインストール認証要求を行い、成功すれば制御部１３０がアンインストールを許可し、揮発性記憶領域１４０に格納された機種固有情報を消去する。

図　3



【特許請求の範囲】
【請求項１】　揮発性記憶領域と不揮発性記憶領域が内蔵されたカートリッジに着脱可能な記録媒体を挿入して、カートリッジ内の不揮発性記憶領域に格納された認証アルゴリズムと、ソフトウェアのインストールプログラムと、ソフトウェアをインストールするシステム装置固有のシステム情報と、記録媒体が持つソフトウェア固有の情報と、カートリッジアクセス装置を利用する事を特徴とするソフトウェアコピーガード実現方法。
【請求項２】　システム装置にアプリケーションをインストールする際、カートリッジ内の不揮発性記憶領域に格納された認証アルゴリズムによる演算結果を揮発性記憶領域に格納されたソフトウェアのライセンス情報に反映する事を特徴とするソフトウェアの不正利用防止方法。
【請求項３】　システム装置内にインストールされた対応アプリケーションを完全に消去する際、カートリッジ内の不揮発性記憶領域に格納された認証アルゴリズムによる演算結果を揮発性記憶領域に格納されたソフトウェアのライセンス情報に反映する事を特徴とするソフトウェア不正利用防止方法。
【請求項４】　請求項２と請求項３の機能を利用して、着脱可能な記録媒体に格納されたソフトウェアをユーザが所持するライセンス数より多いシステム装置へのインストールを防止する特徴を持つソフトウェア不正利用防止方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ソフトウェアの不正利用の防止およびソフトウェアのユーザライセンス管理を行う為に使用する認証方法、着脱可能な記録媒体および装置の技術に関する。
【０００２】
【従来の技術】一般的なパーソナルコンピュータでは、ソフトウェアのインストール時にソフトウェアに付属するソフトウェアのＩＤキーを入力、またはソフトウェアが書き込まれている記録媒体自身にソフトウェア的な処理を施す事によって、ソフトウェアの不正インストール等の防止を行っている。また、ソフトウェアのインストール時にライセンス数の情報等をシステム装置のディスク装置等に書き込む手段等でソフトウェアのライセンス管理を行っていた。
【０００３】
【発明が解決しようとする課題】従来の技術だけでは事前にインストールするソフトウェアのＩＤキーを入手、または記録媒体そのものを複製する手段があれば、不正な方法で入手したソフトウェアでも通常にインストールして利用する事が出来るといった問題があった。また、ソフトウェアのライセンスの管理情報に関してもディスク装置等に書き込む事によるライセンス情報を管理する方法の場合、不正なプログラム等を利用してライセンス管理情報を意図的に改変し、許諾されたライセンス数より多い数のシステム装置で不正利用するケースが考えられる。
【０００４】本発明は、上記の実情を踏まえてソフトウェアのライセンス不正利用を抑止するシステムおよび方法を提供する事を目的とする。
【０００５】
【課題を解決するための手段】課題を解決する為に、アクセス装置の他に複製が難易な不揮発性記憶領域を内蔵したカートリッジを新しく設け、本不揮発性記憶領域内にソフトウェア認証アルゴリズムおよび認証キーを格納し、これらを利用していないとソフトウェアのインストールを不可能にする仕組みを持つソフトウェアの認証を行う。
【０００６】
【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。
【０００７】最初に、認証に必用な各ハードウェアの発明のハードウェア的な実施形態を図１、図２、及び図３を用いて説明する。
【０００８】図１はシステム装置にインストールするソフトウェアを格納した記憶媒体１７０と記録媒体１７０内のソフトウェアを認証する為の中心になるカートリッジ１１０を表している。
【０００９】カートリッジ１７０は着脱可能な記録媒体１７０を格納する記録媒体装着部１６０と、記録媒体１７０に格納されたソフトウェアをシステム装置にインストールまたはアンインストールする際に実行する認証アルゴリズムと認証アルゴリズムに使用する認証キーの両方を格納した不揮発性記憶領域１５０と、対象ソフトウェアをインストールした際に生成される演算結果を格納する揮発性記憶領域１４０と、認証アルゴリズムの処理および揮発性記憶領域１４０と不揮発記憶領域１５０をＩ／Ｏコントロールに関する処理を行う制御部１３０と、後述するカートリッジを読み取るアクセス装置との情報のやり取りを行うカートリッジインターフェース部１２０から構成される。
【００１０】記録媒体１７０をカートリッジ１１０の記録媒体装着部１６０に格納した状態を示すのが図２である。
【００１１】認証アルゴリズムはカートリッジ１１０の不揮発性記憶領域１５０に格納されている為、記憶媒体１７０に格納されたソフトウェアの認証方法を変更するには、現在使用しているカートリッジ１１０を別の認証アルゴリズムを不揮発性記憶領域１５０に格納したカートリッジ１１０と差し替える事によって実現する事が可能である。
【００１２】カートリッジ１１０の不揮発性記憶領域１５０に格納する認証アルゴリズムは同じ入力情報に対し

て必ず同じ演算結果を出力し、異なる入力データに対しては必ず異なる演算結果を出力する必要がある。

【００１３】実際にソフトウェアのインストールとアンインストールを行う際には図２の記録媒体１７０が格納された状態のカートリッジ１１０の他に、カートリッジ１１０とソフトウェアの認証に必用なデータ等をやりとりする為のインターフェース部とカートリッジ１１０の中に格納された記録媒体１７０にアクセスする機能を持つアクセス装置１８０が必用である。

【００１４】着脱可能な記録媒体１７０に格納されたソフトウェアのインストール、またはアンインストールを行う際、記録媒体１７０をカートリッジ１１０の記録媒体装着部１６０に挿入した後に、記録媒体１７０が装着されたカートリッジ１１０をアクセス装置１８０に装着する。

【００１５】ソフトウェアのインストール時の認証処理における発明の処理形態を図３および図４を参照して説明する。

【００１６】ソフトウェアのインストールの際（ステップＳ１０１）には、アクセス装置１８０の制御部１９０はアクセス装置インターフェース部２００とカートリッジ１１０のカートリッジインターフェース部１２０を経て、カートリッジ１１０の制御部１３０に対してインストール認証処理を要求する。

【００１７】インストール認証処理の要求により、カートリッジ１１０の制御部１３０は不揮発性記憶領域１５０に格納された認証キーと、ソフトウェアをインストールするシステム装置の固有情報、および記録媒体１７０の中に格納されたソフトウェア識別キーを取り出して、不揮発性記憶領域１５０内に格納された認証アルゴリズムに従がって演算（ステップＳ１０２）を行い、その演算結果を揮発性記憶領域１４０内に格納されている演算結果のリストと比較して同じ演算結果がリストに存在するか確認（ステップＳ１０３）する。

【００１８】カートリッジ１１０の制御部１３０は、前記の演算結果（ステップＳ１０２）が既に揮発性記憶領域１４０内に格納されていた場合は、ソフトウェアのインストール認証の結果を成功とし、アクセス装置１８０の制御部１９０に対しソフトウェアインストール処理の続行を許可（ステップＳ１０６）する。

【００１９】カートリッジ１１０の制御部１３０は、前記の演算結果（ステップＳ１０２）が揮発性記憶領域１４０内に存在していない状態で、かつ揮発性記憶領域１４０内に演算結果を格納するための領域が残っている場合（ステップＳ１０４）は、演算した結果（ステップＳ１０２）を揮発性記憶領域１４０にライセンス情報として格納した後に（ステップＳ１０５）、ソフトウェアのインストール認証の結果を成功と判断し、アクセス装置１８０の制御部１９０に対して、ソフトウェアインストール処理の続行を許可（ステップＳ１０６）する。

【００２０】カートリッジ１１０の揮発性記憶領域１４０に書き込む事が可能な演算結果（ステップＳ１０５）の領域の上限はインストールするソフトウェアによって許諾されているライセンス数までとする。

【００２１】上記の理由の為、カートリッジ１１０の制御部１３０は、前記の演算結果（ステップＳ１０２）が揮発性記憶領域１４０内に存在していない状態で、かつ揮発性記憶領域１４０内に演算結果を格納するための領域が残っていない場合（ステップＳ１０４）は、ソフトウェアのインストール認証の結果を失敗と判断して、アクセス装置１８０の制御部１９０に対しソフトウェアインストール処理の続行を中断（ステップＳ１０７）させる。

【００２２】あるシステム装置にインストールされたソフトウェアのライセンスを他のシステム装置で利用する等の理由で未使用状態にするには、カートリッジ１１０の揮発性記憶領域１４０内にソフトウェアのライセンス情報として格納されている演算結果を消去する必要がある。この場合、ライセンスを手放すシステム装置の情報が格納されたカートリッジ１１０と、アクセス装置１８０と、対象となるソフトウェアの記録媒体１７０を利用して対象ソフトウェアをアンインストールする必用がある。

【００２３】ソフトウェアのアンインストール時の認証処理における発明の処理形態を図３および図５を参照して説明する。この処理を利用する事でソフトウェアがインストールが許諾されたライセンス数を超えない事を保証する。

【００２４】アンインストール認証処理の要求（ステップＳ２０１）に対しては、カートリッジ１１０の制御部１３０は不揮発性記憶領域１５０に格納された認証キーとソフトウェアをアンインストールするシステム装置の固有情報、および記録媒体１７０に格納されたソフトウェア識別キーを取り出して、不揮発性記憶領域１５０内に格納された認証アルゴリズムに従がって演算（ステップＳ２０２）を行い、導き出された演算結果を揮発性記憶領域１４０内に格納されている演算結果のリストと比較して同じ演算結果が存在するか確認（ステップＳ２０３）する。

【００２５】カートリッジ１１０の制御部１３０は、前記の演算結果（ステップＳ２０２）が揮発性記憶領域１４０内に既に存在している場合は、ソフトウェアのアンインストール認証の結果を成功とし、アクセス装置１８０の制御部１９０に対しソフトウェアのアンインストール処理の続行を許可（ステップＳ２０４）する。そして、ソフトウェアのアンインストール終了後に、導き出した演算結果と同じ内容を揮発性記憶領域１４０に格納された演算結果のリストから消去（ステップＳ２０６）する。

【００２６】カートリッジ１１０の制御部１３０は、前

記の演算結果（ステップＳ２０２）が揮発性記憶領域１４０内が存在していない場合は、ソフトウェアのアンインストール認証の結果を失敗として、アクセス装置１８０の制御部１９０に対しソフトウェアのアンインストールの処理を中断（ステップＳ２０５）する。

【００２７】

【発明の効果】着脱可能な記録媒体内の従来のバイナリ情報を変更する事なく、ソフトウェア利用の抑制およびユーザに許諾されたソフトウェア利用ライセンスの管理を実現する。

【００２８】着脱可能な記録媒体の既存の標準規格との互換性を保持しつつ、ソフトウェアへの対応および利用ソフトウェアのライセンス管理を行うことが可能である。

【００２９】本発明はさらに不揮発性記憶領域内のバイナリ情報を変更する事により着脱可能な記録媒体のバイナリ情報を変更する事なく、必用に応じて認証方法を変更する事が可能である。

【００３０】本発明はカートリッジ内の認証アルゴリズムを利用する事により媒体を特定のシステム装置以外で利用不可能にする事が可能である。

【００３１】本発明はカートリッジ内の複製不可能な不揮発性記憶領域に認証アルゴリズムを格納されており、かつ揮発性記憶領域にソフトウェアのライセンス情報を格納する為、着脱可能な記録媒体を複製された場合でもソフトウェアの不正利用を抑制する事が可能である。

【図面の簡単な説明】

【図１】着脱可能な記録媒体をカートリッジに挿入する図。

【図２】着脱可能な記録媒体がカートリッジに装着された状態を示す図。

【図３】アクセス装置、着脱可能な記録媒体とカートリッジ間のインターフェース及びデータの流れを示す図。

【図４】着脱可能な記録媒体からソフトウェアをインストールする際の認証処理の流れを示す図。

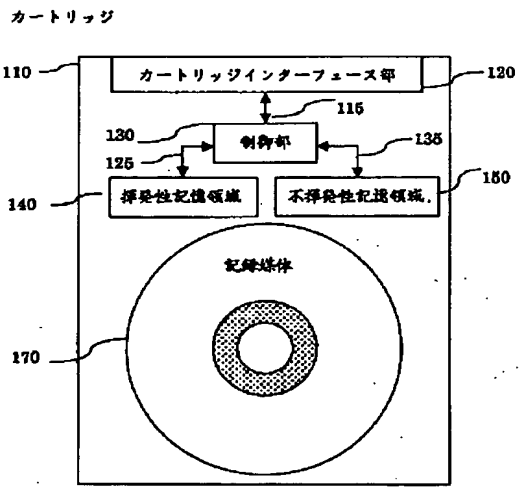
【図５】システム装置からソフトウェアをアンインストールする際の認証処理の流れを示す図。

【符号の説明】

１１０…カートリッジ、１１５…カートリッジインターフェース部と制御部のバス、１２０…カートリッジインターフェース部、１２５…カートリッジ制御部と揮発性記憶領域のバス、１３０…カートリッジ内の処理制御部、１３５…カートリッジ制御部と不揮発性記憶領域のバス、１４０…カートリッジ内揮発性記憶領域、１４５…アクセス装置の制御部とアクセス装置のバス、１５０…カートリッジ内不揮発性記憶領域、１５５…アクセス装置の制御部と着脱可能な記録媒体、１６０…着脱可能な記録媒体の装着部、１７０…着脱可能な記録媒体、１８０…アクセス装置、１９０…アクセス装置制御部、２００…アクセス装置側のカートリッジ媒体へのインターフェース。

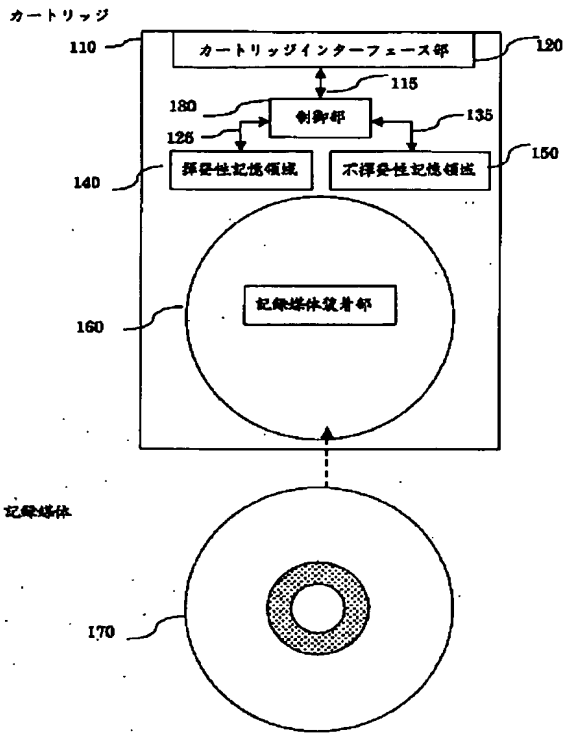
【図２】

図　２



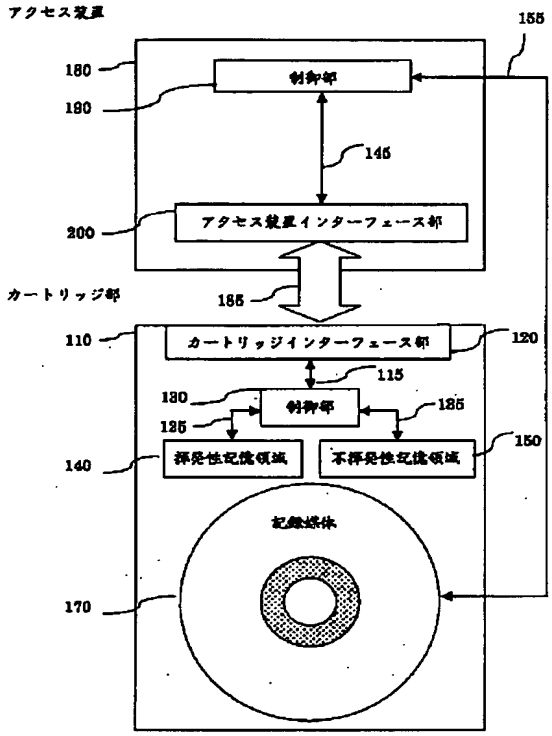
【図１】

図 1


カートリッジ
110
カートリッジインターフェース部
120
115
180
制御部
135
125
揮発性記憶領域
不揮発性記憶領域
150
140
記録媒体装着部
160
記録媒体
170

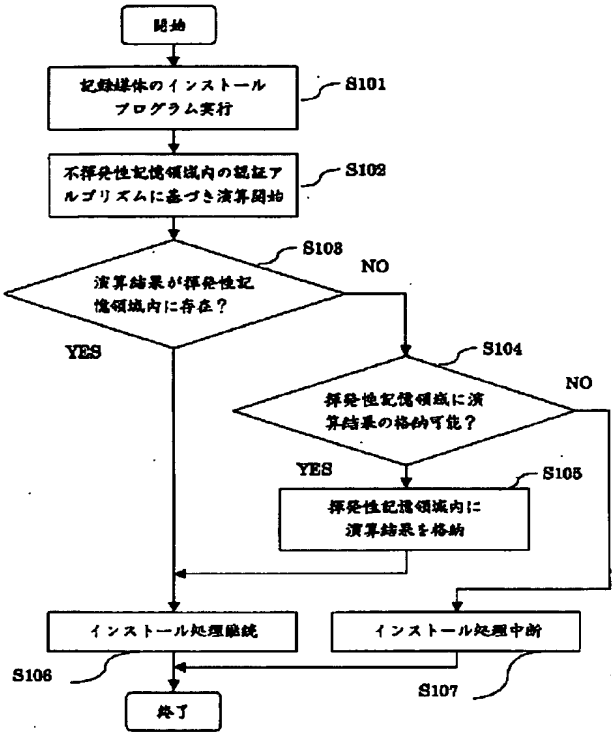
【図３】

図 3


アクセス装置
155
180
制御部
190
145
200
アクセス装置インターフェース部
カートリッジ部
185
110
カートリッジインターフェース部
120
115
130
制御部
125
135
揮発性記憶領域
不揮発性記憶領域
150
140
記録媒体
170

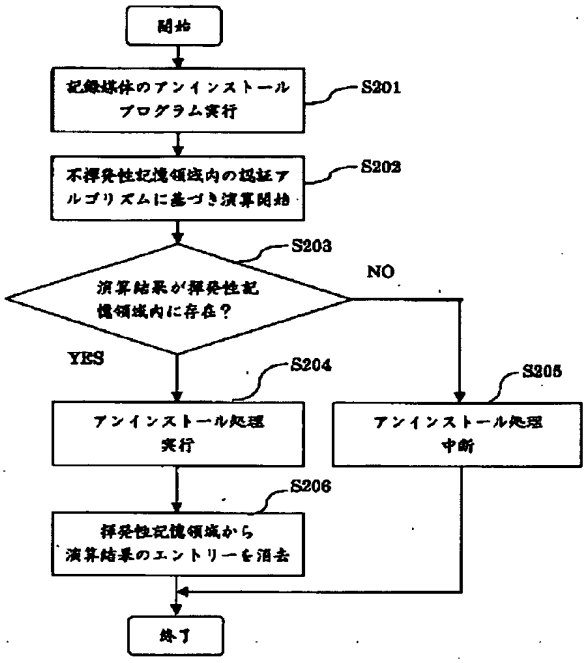
【図４】

図 4


開始
記録媒体のインストール プログラム実行
S101
不揮発性記憶領域内の認証アルゴリズムに基づき演算開始
S102
演算結果が揮発性記憶領域内に存在？
S103
NO
YES
揮発性記憶領域に演算結果の格納可能？
S104
NO
YES
揮発性記憶領域内に演算結果を格納
S105
インストール処理継続
インストール処理中断
S106
S107
終了

【図５】

図 5


開始
記録媒体のアンインストール プログラム実行
S201
不揮発性記憶領域内の認証アルゴリズムに基づき演算開始
S202
演算結果が揮発性記憶領域内に存在？
S203
NO
YES
S204
S205
アンインストール処理実行
アンインストール処理中断
揮発性記憶領域から演算結果のエントリーを消去
S206
終了

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox